

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-261788

(43)Date of publication of application : 13.09.2002

(51)Int.Cl. H04L 12/46  
G06F 13/00  
H04L 12/66

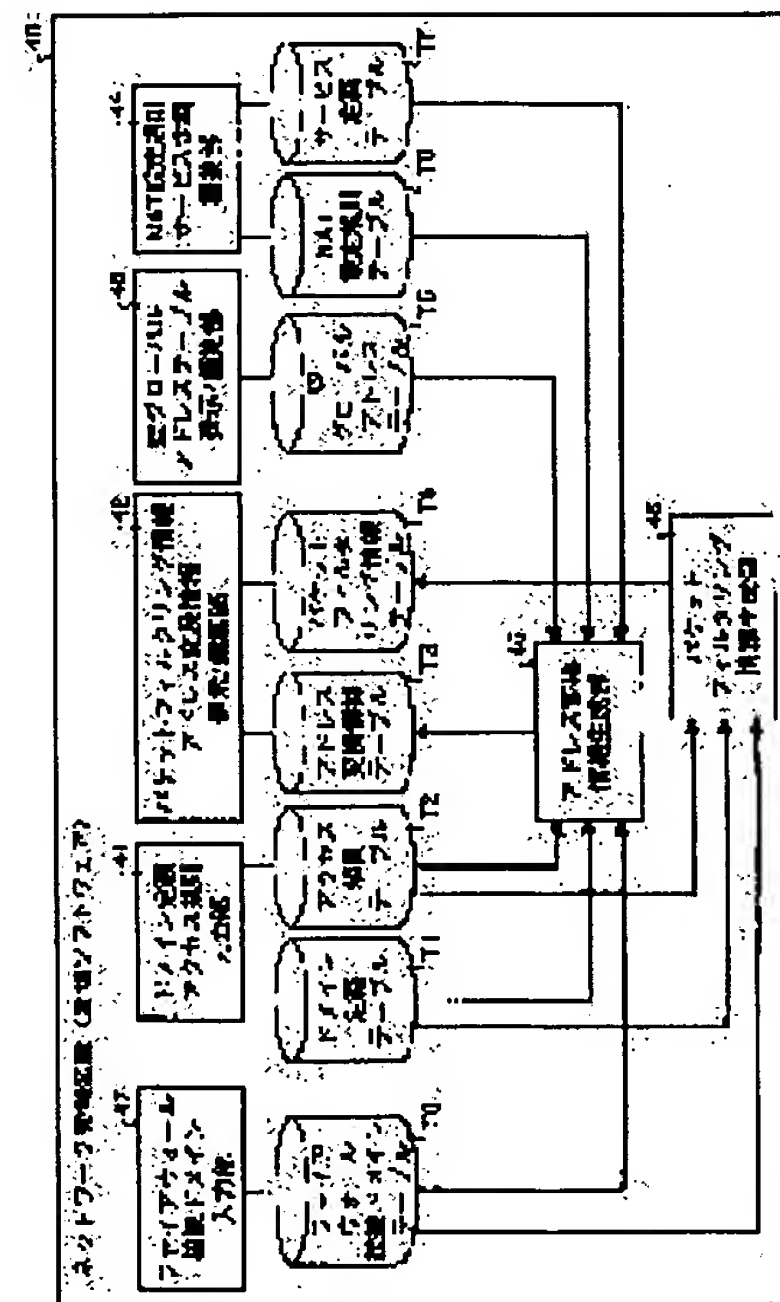
(21)Application number : 2001-052950 (71)Applicant : MITSUBISHI ELECTRIC CORP  
(22)Date of filing : 27.02.2001 (72)Inventor : KANAEGAMI ATSUSHI

## (54) FIREWALL MANAGING APPARATUS AND METHOD

### (57)Abstract:

PROBLEM TO BE SOLVED: To obtain a firewall managing apparatus and a method which can form batch setting information of firewall which includes not only packet filtering information but also address conversion information of an NAT by using definition description easy to be understood by a person, in order to mutually operate a plurality of bases via an internet.

SOLUTION: On the basis of a domain definition table T1 and an access rule table T2 as the operation policy of a LAN 12 and a LAN 13, a vacant global address table T5, an NAT-setting rule table T6 and a service definition table T7, NAT address conversion information D1b, D2b and packet filtering information D1a, D2a are formed by using firewalls FW1, FW2 of the LANs 12, 13.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

BEST AVAILABLE COPY

application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-261788

(P2002-261788A)

(43)公開日 平成14年9月13日(2002.9.13)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト <sup>*</sup> (参考)
H 0 4 L 12/46		H 0 4 L 12/46	E 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 K 0 3 0
H 0 4 L 12/68		H 0 4 L 12/68	B 5 K 0 3 3

審査請求 未請求 請求項の数9 OL (全 15 頁)

(21)出願番号 特願2001-52950(P2001-52950)

(22)出願日 平成13年2月27日(2001.2.27)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 金枝上 敏史

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74)代理人 100089118

弁理士 瀬井 宏明

Fターム(参考) 5B089 DA06 KA17 KB04 KB13

5K030 GA15 HA08 HB08 HC01 HC14

HD06 JL07

5K033 AA08 CB09 DA06 DB18 DB20

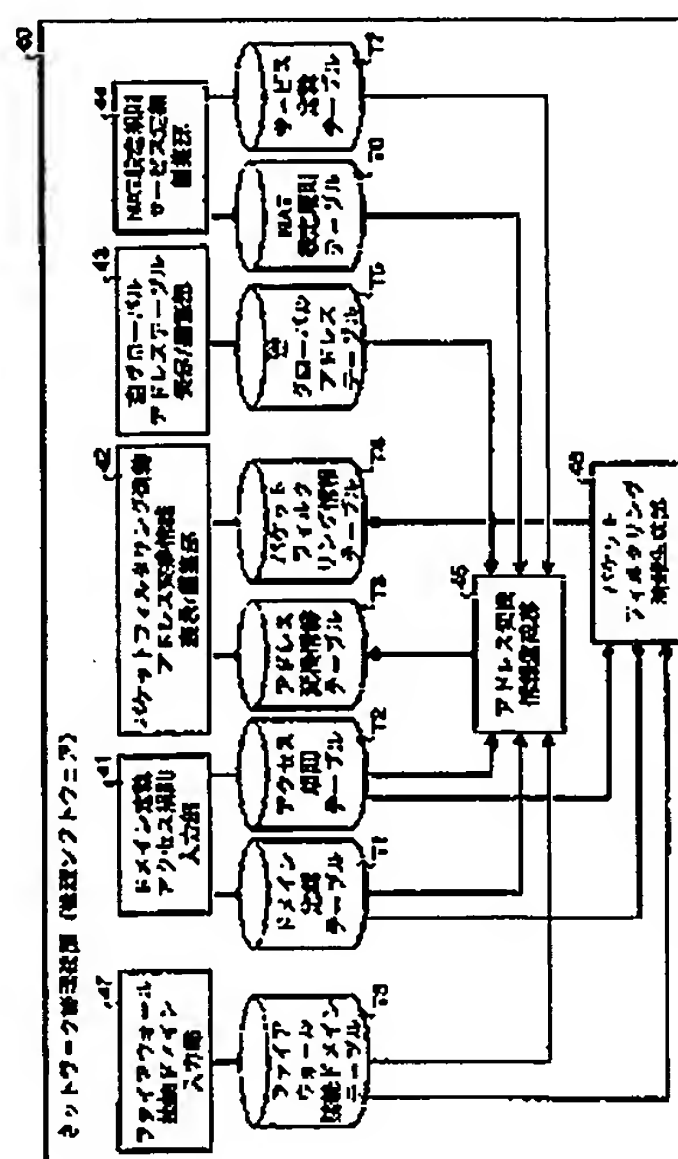
EA07 EC03

(54)【発明の名称】 ファイアウォール管理装置および方法

(57)【要約】

【課題】 インターネットを介して複数拠点間を相互運用するため、人間に判りやすい定義記述を用いてパケットフィルタリング情報だけでなくNATのアドレス変換情報を含めたファイアウォールの設定情報を一括生成し得るファイアウォール管理装置および方法を得ること。

【解決手段】 各LAN12, 13の運用ポリシーとしてのドメイン定義テーブルT1, アクセス規則テーブルT2と、空グローバルアドレステーブルT5と、NAT設定規則テーブルT6と、サービス定義テーブルT7とに基づいて各LAN12, 13のファイアウォールFW1, FW2で用いてNATアドレス変換情報D1b, D2bおよびパケットフィルタリング情報D1a, D2aを生成する。



(2)

特開2002-261788

1

2

【特許請求の範囲】

【請求項1】 NAT機能を有するファイアウォール、1～複数の端末および1～複数のサーバを夫々有する複数のLAN間がインターネットを介して接続されるネットワークに適用され、前記各LANのファイアウォールの設定情報を管理するファイアウォール管理装置において、

前記複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報が予め登録されるデータベースと、

このデータベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのNATアドレス変換情報を作成するアドレス変換情報作成手段と、

前記データベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのパケットフィルタリング情報を作成するパケットフィルタリング作成手段と、を備えることを特徴とするファイアウォール管理装置。

【請求項2】 前記各LANに含まれる端末およびサーバを、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積することと特徴とする請求項1に記載のファイアウォール管理装置。

【請求項3】 前記アクセス規則は、当該LANの1つの端末グループから他のLANの1つのサーバグループへのアクセスをアクセス規則の単位として、管理すべき複数のLAN内に含まれる全ての端末グループおよびサーバグループについて登録されることを特徴とする請求項2に記載のファイアウォール管理装置。

【請求項4】 前記アクセス規則には、前記分けられたグループ毎にグローバルアドレスの割当数が設定されることを特徴とする請求項2または3に記載のファイアウォール管理装置。

【請求項5】 前記アクセス規則には、各アクセス規則毎に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されることを特徴とする請求項3または4に記載のファイアウォール管理装置。

【請求項6】 前記NAT設定規則には、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無が登録され、NAT設定規則はこれら3つの登録情報に基づいてNAT種別を分類することを特徴とする請求項2～5のいずれか一つに記載のファイアウォール管理装置。

【請求項7】 前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されていることを特徴とする請求項2～6のいずれか一つに記載のファイアウォール管理装置。

【請求項8】 前記運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレ

ス、NAT設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えることを特徴とする請求項1～7のいずれか一つに記載のファイアウォール管理装置。

【請求項9】 NAT機能を有するファイアウォール、1～複数の端末および1～複数のサーバを夫々有する複数のLAN間がインターネットを介して接続されるネットワークに適用され、前記各LANのファイアウォールの設定情報を管理するファイアウォール管理方法において、

前記複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を予め登録するステップと、

このデータベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのNATアドレス変換情報およびパケットフィルタリング情報を作成するステップと、

を備えることを特徴とするファイアウォール管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、NAT機能を有するファイアウォールの設定情報を自動作成するための技術に関し、特にインターネットを介した複数のLAN（ローカルエリアネットワーク）間を接続するための運用ポリシーなどに基づいて各LANにおけるファイアウォールのアドレス変換情報およびパケットフィルタリング情報を作成するファイアウォール管理装置および方法に関するものである。

【0002】

【従来の技術】運用ポリシーからファイアウォールの設定情報を生成する技術は、ポリシーネットワークングとして近年注目を集めている。

【0003】従来、ファイアウォールの管理のためには、多数の運用ポリシーの管理が必要であり、そのためにはネットワークの高度な技術やベンダ固有の設定情報の習得を必要とする。また、ファイアウォールへの設定情報から第三者が網の運用ポリシーを理解するのは困難であった。

【0004】そこで、ファイアウォールの運用ポリシーを管理する技術として、特開2000-253066号公報の「ファイアウォールを管理するための方法および装置」がある。この従来技術では、イントラネットのトポロジーとファイアウォールの運用規則の関係を表わすエンティティ関係モデルと、運用規則のインスタンスを定義するモデル定義言語とから、ファイアウォールに設定するコンフィギュレーションファイルの生成を実現している。この技術によれば、運用規則とトポロジーを独立に管理することができ、トポロジーが変更されても運用規則を置き換える必要がなく、運用ポリシーの再利用が可能とな

(3)

特開2002-261788

3

4

る。この従来技術では、生成される設定情報は、パケットフィルタリングとフィルタリングの優先度に関するものしかない。

【0005】また、特開2000-24495号公報の「ネットワーク管理システム」には、独立性を保って定義した運用規則と網トポロジとからファイアウォールやルータの設定情報を生成することが開示されており、ファイアウォールの規則の複雑さ、規則の順番、他の設定情報との整合性を意識せずに管理者がセキュリティポリシーを設計できるようにしている。また、セキュリティポリシーを装置固有の設定情報のシンクタスおよびセマンタクスから分離することにより、ポリシー定義情報の共有および再利用を可能とすることが示されている。

【0006】

【発明が解決しようとする課題】しかしながら、これらの従来技術には、LAN内での運用ポリシーを管理することしか開示されておらず、インターネットを介した複数のLAN間での運用ポリシーを統括して管理することは何ら開示されていない。このようなインターネットを介した複数のLAN間での運用ポリシーの管理に対する要求は、専用線を待たずに離れた複数の拠点間をインターネットを介して相互運用したい状況下で発生する。

【0007】近年、IPアドレスの枯渇を解決するために、スタブドメインの境界にNAT（Network Address Translation ネットワークアドレス変換）を置くことが提案されている。NATは、LAN内だけで用いられるローカルアドレス（プライベートアドレス）とインターネットで用いられるグローバルにユニークなグローバルアドレスとの間でアドレス変換する技術である。そして、ファイアウォールにもNAT機能を付加機能として設けることが提案されている。

【0008】NATを用いて複数のLAN間を接続するための管理装置を提供するためには、上記従来技術のようなパケットフィルタリング情報だけでなく、NATで用いられるローカルアドレスとグローバルアドレスのアドレス変換情報をファイアウォールに設定する必要がある。

【0009】しかしながら、前述したように、上記従来技術では、LAN内での運用ポリシーを管理するべく主にパケットフィルタリング情報を生成することしか開示されておらず、インターネットを介した複数のLAN間で運用ポリシーを管理するためにパケットフィルタリング情報のみならずNATのアドレス変換情報を生成することは開示されていない。

【0010】この発明は上記に鑑みてなされたもので、インターネットを介して複数拠点間を相互運用するため、人間に判りやすい定義記述を用いてパケットフィルタリング情報だけでなくNATのアドレス変換情報を含めたファイアウォールの設定情報を生成することができファイアウォール管理装置および方法を得ることを目

的としている。

【0011】

【課題を解決するための手段】上記目的を達成するためこの発明では、NAT機能を持つファイアウォール、1～複数の端末および1～複数のサーバを夫々有する複数のLAN間がインターネットを介して接続されるネットワークに適用され、前記各LANのファイアウォールの設定情報を管理するファイアウォール管理装置において、前記複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報が予め登録されるデータベースと、このデータベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのNATアドレス変換情報を作成するアドレス変換情報作成手段と、前記データベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのパケットフィルタリング情報を作成するパケットフィルタリング作成手段とを備えることを特徴とする。

【0012】この発明によれば、複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を用いてNATアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、NATを用いて複数のLAN間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【0013】つぎの発明によれば、上記発明において、前記各LANに含まれる端末およびサーバを、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積すること特徴とする。

【0014】この発明によれば、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積している。

【0015】つぎの発明によれば、前記アクセス規則は、当該LANの1つの端末グループから他のLANの1つのサーバグループへのアクセスをアクセス規則の単位として、管理すべき複数のLAN内に含まれる全ての端末グループおよびサーバグループについて登録されることを特徴とする。

【0016】この発明によれば、当該LANの1つの端末グループから他のLANの1つのサーバグループへのアクセスを単位として、アクセス規則を登録している。

【0017】つぎの発明によれば、上記発明において、前記アクセス規則には、前記分けられたグループ毎にグローバルアドレスの割当数が設定されることを特徴とする。

【0018】この発明によれば、アクセス規則にグローバルアドレスの割当数がグループ毎に設定している。



(4)

特開2002-261788

5

【0019】つぎの発明によれば、上記発明において、前記アクセス規則には、各アクセス規則毎に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されることを特徴とする。

【0020】この発明によれば、アクセス規則には、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されている。

【0021】つぎの発明によれば、上記発明において、NAT設定規則には、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無が登録され、NAT設定規則はこれら3つの登録情報に基づいてNAT種別を分類することを特徴とする。

【0022】この発明によれば、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無に基づいてNAT種別が分類される。

【0023】つぎの発明によれば、上記発明において、前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されていることを特徴とする。

【0024】この発明によれば、前記サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されている。

【0025】つぎの発明によれば、上記発明において、前記運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えることを特徴とする。

【0026】この発明によれば、上記の各種情報を編集し、該編集結果を前記データベースに登録する手段を備えているので、運用ポリシー、LANの構成などが変更された場合にもこれに容易に対処することができる。

【0027】つぎの発明によれば、NAT機能を持つファイアウォール、1～複数の端末および1～複数のサーバを夫々有する複数のLAN間がインターネットを介して接続されるネットワークに適用され、前記各LANのファイアウォールの設定情報を管理するファイアウォール管理方法において、前記複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を予め登録するステップと、このデータベースに蓄積された情報に基づいて前記複数のLANの各ファイアウォールのNATアドレス変換情報およびパケットフィルタリング情報を作成するステップとを備えることを特徴とする。

【0028】この方法発明によれば、複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、

5

サービス定義に関する情報を用いてNATアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、NATを用いて複数のLAN間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【0029】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるファイアウォール管理装置および方法の好適な実施の形態を詳細に説明する。

【0030】実施の形態1 初めに、本発明の対象とするネットワーク構成の一例を説明する。図1はNAT機能とパケットフィルタリング機能を持つファイアウォールFW1およびFW2を用い、インターネット11を介して2つのLAN12、13を接続した網構成を示すものである。

【0031】ファイアウォールFW1（ファイアウォール1）の内部でローカルエリアネットワークを構成するLAN12およびファイアウォールFW2（ファイアウォール2）の内部でローカルエリアネットワークを構成するLAN13は、例えば、夫々、同じ会社の距離の離れた工場で構成されたネットワークである。LAN接続された各工場は、協力して製品開発をおこなっており、それぞれの工場の設計担当者は端末パソコンを用いて設計作業をおこない、工場間の設計者間では、インターネット11を介して設計データの交換を可能としているものとする。

【0032】LAN12、13は、IPアドレスをローカルアドレス（プライベートアドレス）で管理しており、インターネット11はIPアドレスを勿論グローバルアドレスで管理している。

【0033】ファイアウォールFW1は、LAN12内とインターネット11との間でどのパケットを通過させるか否かを所定の規則に従って判定するパケットフィルタリング機能を有するとともに、インターネット11からLAN12内のローカルアドレスを隠蔽するため、パケット内のIPアドレスを変換するNAT機能を有している。ファイアウォールFW1においては、後述するネットワーク管理装置の管理ソフトウェア40によって作成されたパケットフィルタリング情報D1aおよびアドレス変換情報D1bが蓄積記憶されており、これらの情報D1aおよびD1bに基づいてパケットフィルタリング機能およびNAT機能を実行する。ファイアウォールFW2も同様であり、後述するネットワーク管理装置の管理ソフトウェア40によって作成されたパケットフィルタリング情報D2aおよびアドレス変換情報D2bが蓄積記憶されており、これらの情報D2aおよびD2bに基づいてパケットフィルタリング機能およびNAT機能を実行する。

【0034】この場合、LAN12内には、2つのクライアント端末（以下単に端末という）21、22と2つ

(5)

特開2002-261788

7

のサーバ23、24とが含まれている。クライアント端末21、22は1つの端末ドメイン14（端末ドメインAともいう）に属し、サーバ23、24は、1つのサーバドメイン15（サーバドメインBともいう）に属している。この場合は、便宜上1つの端末ドメインAおよびサーバドメインAしか示していないが、通常は1〜複数の端末ドメインおよびサーバドメインが含まれる。

【0035】LAN13内には、この場合、2つのクライアント端末31、32と2つのサーバ33、34とが含まれている。クライアント端末31、32は1つの端末ドメイン16（端末ドメインBともいう）に属し、サーバ33、34は、1つのサーバドメイン17（サーバドメインBともいう）に属している。LAN13にも、通常は、1〜複数の端末ドメインおよびサーバドメインが含まれる。

【0036】通常、各LAN12、13には、複数のホスト（端末およびサーバ）が含まれているが、これら複数のホストを端末とサーバとを別グループとして、任意の複数のグループに分け、これら分けた1つのグループを本明細書中ではドメインと呼称している。したがって、分割された1つのグループに1つのドメイン名が割り振られる。上記グループ（ドメイン）の単位は、例えば、工場内の経理グループ、総務グループ、技術グループなどであり、業務種別によって分けたグループ毎に所定のドメイン名が割り振られる。したがって、この場合、LAN12には、ドメイン名が端末ドメインAである端末ドメイン14とドメイン名がサーバドメインAであるサーバドメイン15との2つのグループ（ドメイン）が存在し、LAN13には、ドメイン名が端末ドメインBである端末ドメイン16とドメイン名がサーバドメインBであるサーバドメイン17との2つのグループ（ドメイン）が存在している。

【0037】LAN12内の各ホスト（端末21、22およびサーバ23、24）には、図1に示すように、当該LAN内で一意なローカルIPアドレスL1〜L4がそれぞれ割り振られており、また、LAN13内の各ホスト（端末31、32およびサーバ33、34）には、当該LAN内で一意なローカルIPアドレスL101〜L104が夫々割り振られている。

【0038】この図1の網構成では、以下の3種類のNAT機能を持つものとする。

#### 【0039】Basic NAT

IPアドレスを対象としたアドレス変換方式であり、割当IPアドレスとして、アドレス変換規則に指定された割当IPアドレス範囲のなかの空きIPアドレスが動的に割り当てられる。同一ローカルIPアドレスを端点とする通信フローは同一の割当IPアドレスを共有する。

#### 【0040】Static NAT

グローバルIPアドレスとローカルIPアドレスの変換の組合せをスタティックに決める。サーバのようにグロ

8

ーバルアドレスを固定しなくてはならないときに用いる。

#### 【0041】NAPT

IPアドレスおよびTCP（UDP）ポート番号を変換対象としたアドレス変換方式であり、ローカルIPアドレスとグローバルIPアドレスとの間で多対1の変換を可能にする方式がある。このNAPT方式は、同じグローバルアドレスの複数のポート番号にローカルIPアドレスを割り当てる。

10 【0042】図2はファイアウォールFW1、FW2への設定情報を生成するネットワーク管理装置（ファイアウォール管理装置）に内蔵される管理ソフトウェア40の機能構成の一例を示したものである。

20 【0043】図2において、ドメイン定義アクセス規則入力部41、パケットフィルタリング情報アドレス変換情報表示／編集部42、空グローバルアドレステーブル表示／編集部43、NAT設定規則サービス定義編集部44、ファイアウォール接続ドメイン入力部47は、管理者と各テーブルT1〜T8とのインタフェースである。

【0044】ドメイン定義テーブルT1、アクセス規則テーブルT2、アドレス変換情報テーブルT3、パケットフィルタリング情報テーブルT4、空グローバルアドレステーブルT5、NAT設定規則テーブルT6、サービス定義テーブルT7およびファイアウォール接続ドメインテーブルT8は、各種テーブルを格納するデータベースである。

30 【0045】アドレス変換情報生成部45およびパケットフィルタリング情報生成部46は、ファイアウォールFW1およびFW2の設定情報（アドレス変換情報およびパケットフィルタリング情報）を生成するプログラムである。

【0046】以下、個々の詳細について説明する。ドメイン定義アクセス規則入力部41は、ドメイン定義テーブルT1およびアクセス規則テーブルT2に対し、ドメイン定義およびアクセス規則を入出力するための管理者とのインタフェースである。管理者は、このドメイン定義アクセス規則入力部41を介して当該網構成すなわちインターネット11を介して接続されるLAN11、12の運用ポリシーを定義する。

40 【0047】パケットフィルタリング情報アドレス変換情報表示／編集部42は、作成されたアドレス変換情報テーブルT3のアドレス変換情報およびパケットフィルタリング情報テーブルT4のパケットフィルタリング情報を表示および編集するためのユーザインタフェースであり、編集の結果は再びアドレス変換情報テーブルT3およびパケットフィルタリング情報テーブルT4に格納される。

50 【0048】空グローバルアドレステーブル表示／編集部43は、各LAN12、13に割当て可能な空グロ

(5)

特開2002-261788

9

10

バルアドレスを管理するためのユーザインタフェースであり、空グローバルアドレスの表示、追加、削除を行う。空グローバルアドレスの編集結果は、空グローバルアドレステーブルT5に登録される。

【0049】NAT設定規則サービス定義編集部44は、NAT設定規則およびサービス定義情報を表示編集するためのインタフェースであり、それらの編集結果をNAT設定規則テーブルT6、サービス定義テーブルT7に蓄積する。

【0050】ファイアウォール接続ドメイン入力部47は、各ファイアウォールFW1、FW2に接続される接続ドメインをファイアウォール接続ドメインテーブルT8に登録、編集するためのインタフェースである。

【0051】ファイアウォール接続ドメインテーブルT8には、図3に示すように、各ファイアウォールFW1、FW2に接続される接続ドメインがファイアウォールFW1、FW2毎に登録される。この場合、図1に示すように、ファイアウォールFW1には、端末ドメインAおよびサーバドメインAが接続され、またファイアウォールFW2には、端末ドメインBおよびサーバドメインBが接続される。

【0052】ドメイン定義テーブルT1には、図4に示すように、インターネット11を介した2つのLAN12および13のドメイン定義が蓄積記憶される。このドメイン定義には、ドメイン（ドメイン名、グループ）毎に、ドメイン種別（端末かサーバかの区別）と、当該ドメインに割り振られたホストアドレス（ローカルIPアドレス）とが登録される。このドメイン定義は、図5に示すアクセス規則（アクセス定義）と共に、管理者が、各LAN12、13で用いる運用ポリシーとして、予め定義する。例えば、ドメイン名が端末ドメインAである場合は、ドメイン種別は端末であり、このドメインAには、ローカルIPアドレスがL1、L2である2つの端末が含まれることになる。

【0053】アクセス規則テーブルT2には、図5に示すように、インターネット11を介した2つのLAN12および13のアクセス規則が記憶される。このアクセス規則は、図4に示したドメイン定義と共に、管理者が、各LAN12、13で用いる運用ポリシーとして、予め定義する。アクセス規則は、必要な複数のアクセス規則から成る。すなわち、アクセス規則は、当該LANの1つの端末ドメインから他のLANの1つのサーバドメインへのアクセスをアクセス規則の単位（1つの規則名）として、管理すべき複数のLAN内に含まれる全ての端末グループおよびサーバグループについて登録される。各アクセス規則には、規則名（この場合、PJ1-1、PJ1-2の2つの規則名）、適用ドメインfrom（端末側ドメイン）、適用ドメインto（サーバ側ドメイン）、用いるプロトコル種別（この場合はTCP）、可能なサービス種別（この場合はFTP）、ドメイン内での

の複数の同時接続の有無が含まれている。適用ドメインfromには、ドメイン名と割り当てアドレス数（割り当て可能なグローバルIPアドレス数）が含まれている。適用ドメインtoには、ドメイン名、割り当てアドレス数（割り当て可能なグローバルIPアドレス数）が含まれている。この場合は、端末ドメインAおよびBの割り当てアドレス数は夫々1である。サーバドメインには、当該サーバドメインに含まれるサーバ数分のグローバルIPアドレスが必要なので、サーバドメインの割り当てアドレス数はこのテーブルT2では登録されていない。

【0054】空グローバルアドレステーブルT5には、図6に示すように、各ファイアウォールFW1、FW2毎に割り当て可能な空グローバルIPアドレスが記憶される。この場合、ファイアウォールFW1には、複数のグローバルIPアドレスG1、G2、…が割り振られ、ファイアウォールFW2には、複数のグローバルIPアドレスG101、G102、…が割り振られている。このテーブルT5も、管理者が予め作成登録する。

【0055】NAT設定規則テーブルT6は、図7に示すように、上記した3つのNAT種別のうちの1つを選択するための規則が設定されたテーブルである。このテーブルT6も、管理者が予め作成登録するものであり、この登録内容に応じてアドレス変換情報生成部45での後述する処理手順（アルゴリズム）が決定される。図7の場合は、ドメイン種別が端末で、自ドメイン内での複数同時接続があり、サービス指定ポート番号がある場合、あるいは、ドメイン種別が端末で、自ドメイン内での複数同時接続がなしで、サービス指定ポート番号がある場合は、Basic NATが選択される。ドメイン種別が端末で、自ドメイン内での複数同時接続があり、サービス指定ポート番号がない場合、あるいは、ドメイン種別が端末で、自ドメイン内での複数同時接続がなしで、サービス指定ポート番号がない場合は、NAPTが選択される。ドメイン種別がサーバである場合は、Static NATが選択される。

【0056】サービス定義テーブルT7には、図8に示すように、サービス種別（この場合はFTPのみ）および指定ポート番号の有無ならびに指定ポート番号の内容が設定される。この場合は、FTPの場合は、ドメイン種別が端末のときは、ポート番号の指定はなしとし、ドメイン種別がサーバのときは、2つのポート番号が設定されるようにしている。このテーブルT7も、管理者が予め作成登録する。

【0057】アドレス変換情報生成部45は、NATアドレス変換情報の生成手順が実装されたプログラムであり、ドメイン定義テーブルT1に記憶されたドメイン定義、アクセス規則テーブルT2に記憶されたアクセス規則、空グローバルアドレステーブルT5に記憶内容、NAT設定規則テーブルT6に記憶されたNAT設定規則、サービス定義テーブルT7に記憶されたサービス定



(7)

特開2002-261788

11

義に基づいてファイアウォールFW1およびFW2のNATアドレス変換情報を作成し、該作成したアドレス変換情報をアドレス変換情報テーブルT3に記憶する。

【0058】アドレス変換情報テーブルT3には、図10および図11に示すような、アドレス変換情報生成部45によって作成されたファイアウォールFW1およびFW2のNATアドレス変換情報が記憶される。このアドレス変換情報テーブルT3の記憶内容は、パケットフィルタリング情報アドレス変換情報表示/編集部42を介して管理者が適宜編集することができる。

【0059】パケットフィルタリング情報生成部46は、ファイアウォールFW1およびFW2のパケットフィルタリング情報の生成手順が実装されたプログラムであり、ドメイン定義テーブルT1に記憶されたドメイン定義、アクセス規則テーブルT2に記憶されたアクセス規則に基づいてファイアウォールFW1およびFW2のパケットフィルタリング情報を作成し、該作成したパケットフィルタリング情報をパケットフィルタリング情報テーブルT4に記憶する。

【0060】パケットフィルタリング情報テーブルT4には、図15、図16に示すように、パケットフィルタリング情報生成部46によって作成されたファイアウォールFW1およびFW2のパケットフィルタリング情報が記憶される。このパケットフィルタリング情報テーブルT4の記憶内容は、パケットフィルタリング情報アドレス変換情報表示/編集部42を介して管理者が適宜編集することができる。

【0061】図9は、アドレス変換情報生成部45によって行なわれるNATアドレス変換情報の作成手順を示すものである。以下、この作成手順の詳細を説明する。

【0062】図9の手順の前に、アドレス変換情報生成部45は、図3に示すファイアウォール接続ドメインテーブルT8の登録内容を読み出すことにより、今回のアドレス変換情報作成処理を行うファイアウォール（この場合は2つのファイアウォールFW1およびFW2）と、これらファイアウォールに接続されるドメインに関する登録内容を認知している。

【0063】まず、図5に示すアクセス規則テーブルT2の登録アクセス規則から1つのアクセス規則（例えば規則名PJ1-1）を取り出し（ステップS101）、さらに取り出したアクセス規則からこのアクセス規則に属する適用ドメインfromあるいは適用ドメインtoを取り出す（ステップS102）。そして、図4に示すドメイン定義テーブルT1の内容も参照することにより、取り出した適用ドメインfrom（あるいはto）のドメイン名（例えば端末ドメインA）に対応するドメイン種別が端末であるかサーバであるかを判定する（ステップS103）。

【0064】ステップS103の判定の結果がサーバである場合は、NAT種別をStatic NATとする（ステップ

12

S108）。このNAT種別の選択は、図7に示したNAT設定規則テーブルT6の登録内容に基づいて行われている。

【0065】ステップS103の判定の結果が端末である場合は、つぎに、取り出したアクセス規則における複数同時接続の有無の欄（図5参照）を参照することにより、ドメイン内での同時接続があるか否かを判定する（ステップS104）。この判定の結果、同時接続が行われない場合は、NAT種別をBasic NATとする（ステップS109）。

【0066】ステップS104で同時接続があると判定された場合は、つぎに、取り出したアクセス規則の適用ドメインfrom（あるいはto）の割当アドレス数の欄（図5参照）を参照することにより、当該ドメインに複数のグローバルアドレスを割り当てているか否かを判定する（ステップS105）。当該ドメインに複数のグローバルアドレスを割り当てていると判定された場合は、NAT種別をBasic NATとする（ステップS109）。

【0067】ステップS105で、当該ドメインに複数のグローバルアドレスを割り当てていないと判定された場合は、つぎに、図8に示したサービス定義テーブルT7の登録内容も参照して、利用されるサービス種別（この実施例ではFTP）にポート番号指定があるか否かを判定する（ステップS106）。

【0068】ステップS106でポート番号指定があると判定された場合は、NAT種別をBasic NATとする（ステップS109）。また、ステップS106でポート番号指定がないと判定された場合は、NAT種別をNAPTとする（ステップS107）。

【0069】上述のような処理によって、手順がステップS107に移行されて、NAT種別としてNAPTが選択された場合は、図6に示した空グローバルアドレステーブルT5から1個のグローバルアドレスを取り出し、該取り出した1個のグローバルアドレスをテーブルT5から削除する（ステップS110）。この場合、端末ドメインBの場合は、NAPTが選択されることになるので、端末ドメインBには1つのグローバルアドレスが割当てられることになる。

【0070】また、手順がステップS109に移行されて、NAT種別としてBasic NATが選択された場合は、当該読み出されたアクセス規則の適用ドメインfrom（あるいはto）の当該ドメイン名に対応する割当アドレス数を参照することにより、図6に示した空グローバルアドレステーブルT5から前記割当アドレス数分のグローバルアドレスを先頭から順に取り出し、該取り出した1～複数のグローバルアドレスをテーブルT5から削除する（ステップS111）。この場合、端末ドメインAの場合は、Basic NATが選択されるが、図5のアクセス規則テーブルT2によれば、端末ドメインAの割当アドレス数は1であるので、1個のグローバルアドレスが空グロ

(8)

特開2002-261788

13

ーバルアドレステーブルT5から取り出される。

【0071】また、手順がステップS108に移行されて、NAT種別としてStatic NATが選択された場合は、図5のアクセス規則テーブルT2および図4のドメイン定義テーブルT1を参照することにより、図6に示した空グローバルアドレステーブルT5から当該ドメイン

(この場合はサーバ端末)のホスト数(サーバ数)分のグローバルアドレスを先頭から順に取り出し、該取り出した1〜複数のグローバルアドレスをテーブルT5から削除する(ステップS112)。この場合、サーバドメ

インAの場合は(サーバドメインBも)、Static NATが選択されるが、図4のドメイン定義テーブルT1によれば、サーバドメインAのホスト数は2であるので、2個のグローバルアドレスが空グローバルアドレステーブルT5から取り出される。

【0072】このようなグローバルアドレスの取り出しの際、上記の場合は、グローバルアドレスを空グローバルアドレステーブルT5から早い者順に先頭から取り出すようにしているが、グローバルアドレスの割り当てのための所定の規則を作り、指定されたグローバルアドレスが既に割り当てられているか否かを管理するデータベースを作成してもよい。

【0073】ステップS107〜S109の何れかの手順が終了すると、取り出した適用ドメインに属するホストアドレス(ローカルアドレス)を図4に示したドメイン定義テーブルT1から取り出し、この取り出されたホストアドレス(ローカルアドレス)を先の手順で取り出されたグローバルアドレスおよびNAT種別に対応付けて、ローカルアドレス(ポート番号も用いる場合はポート番号も付加する)、グローバルアドレスおよびNAT種別を項目として含む図10および図11に示すようなアドレス変換情報を作成し、該作成したアドレス変換情報をアドレス変換情報テーブルT3に記憶する(ステップS113)。

【0074】つぎに、同じアクセス規則に他の適用ドメインがあるか否かを判定する(ステップS114)。すなわち、先の手順で適用ドメインfromが選択されていたときには、この段階で、他方の適用ドメインtoが選択されることになる。そして、選択された適用ドメインに対し、前述したステップS103〜ステップS113の手順が実行されることにより、当該適用ドメインに対応するアドレス変換情報が作成され、作成されたアドレス変換情報はアドレス変換情報テーブルT3に記憶される。

【0075】当該アクセス規則に属する2つの適用ドメイン(適用ドメインfromおよび適用ドメインto)に関するアドレス変換情報作成処理が終了すると、ステップS114の判断はNOになり、手順はステップS115に移行される。

【0076】ステップS115においては、図5に示すアクセス規則テーブルT2につぎのアクセス規則がある

14

か否かが判定される。次のアクセス規則がある場合は、このアクセス規則に含まれる2つの適用ドメインについて、1つずつ、前述したステップS103〜ステップS113の手順が実行されることにより、当該アクセス規則に含まれる2つの適用ドメインについてのアドレス変換情報が作成され、作成された各アドレス変換情報は前記同様にしてアドレス変換情報テーブルT3に記憶される。

【0077】図5のアクセス規則テーブルT2に登録された全てのアクセス規則について、前述した処理を繰り返すことにより、図10および図11に示すような、各LAN12、13のファイアウォールFW1、FW2のアドレス変換情報が作成される。そして、このようなアドレス変換情報の作成によって、図3のドメイン定義テーブルT1に、図12に示すように、グローバルアドレスが付加されたものが追加される。

【0078】図10は、ファイアウォールFW1のアドレス変換情報である。ローカルアドレスL1、L2は、グローバルアドレスG1にBasic NATによってアドレス変換される。ローカルアドレスL3は、グローバルアドレスG3にStatic NATによってアドレス変換される。ローカルアドレスL4は、グローバルアドレスG4にStatic NATによってアドレス変換される。

【0079】図11は、ファイアウォールFW2のアドレス変換情報である。ローカルアドレスL101、L102は、グローバルアドレスG101にNAPTによってアドレス変換される。ローカルアドレスL103は、グローバルアドレスG103にStatic NATによってアドレス変換される。ローカルアドレスL104は、グローバルアドレスG104にStatic NATによってアドレス変換される。

【0080】図12においては、端末ドメインAの欄にグローバルアドレスG1が付加され、サーバドメインAの欄に2つのグローバルアドレスG3、G4が付加され、端末ドメインBの欄にグローバルアドレスG101が付加され、サーバドメインBの欄に2つのグローバルアドレスG103、G104が付加されている。

【0081】図13および図14は、パケットフィルタリング情報生成部46によって行なわれるパケットフィルタリング情報の作成手順を示すものである。以下、この作成手順の詳細を説明する。

【0082】まず、図5に示すアクセス規則テーブルT2から1つのアクセス規則(例えば規則名PJ1-1)を取り出す(ステップS201)。

【0083】つぎに、取り出したアクセス規則からこのアクセス規則に属する適用ドメインfromを取り出し(ステップS202)、この適用ドメインfromのドメイン名に対応する1〜複数のホストアドレス(ローカルアドレス)を図4のドメイン定義テーブルT1から取り出す(ステップS203)。

(9)

特開2002-261788

15

【0084】つぎに、先に取り出したアクセス規則に属する適用ドメインtoを取り出し（ステップS204）、この適用ドメインtoのドメイン名に対応する1～複数のホストアドレス（グローバルアドレス）を図12のドメイン定義テーブルT1から取り出す（ステップS205）。

【0085】つぎに、適用ドメインfromの1～複数のホストアドレス（ローカルアドレス）を発信元アドレス/ポート番号とし、適用ドメインtoの1～複数のホストアドレス（グローバルアドレス）を宛先アドレス/ポート番号とした全てのホストアドレスの組み合わせを何れかのファイアウォールのパケットフィルタリング情報としてパケットフィルタリング情報テーブルT4に登録する（ステップS206）。

【0086】図5の規則名PJ1-1の場合は、適用ドメインfrom（端末ドメインA）のホストアドレス（ローカルアドレス）がL1、L2で、適用ドメインto（サーバドメインB）のホストアドレス（グローバルアドレス）がG103、G104であるので、L1→G103、L1→G104、L2→G103、L2→G104の4つのパケットフィルタリング情報がファイアウォールFW1用のものとして登録される。これら4つのパケットフィルタリング情報は、図15の上側の4つの欄に示されている。

【0087】つぎに、上記取り出したアクセス規則のプロトコル種別を図5に示すアクセス規則テーブルT2から取り出し、該取り出したプロトコル種別を上記登録したパケットフィルタリング情報にプロトコル種別として登録する（ステップS207）。

【0088】さらに、登録したパケットフィルタリング情報に通信の方向（例えば双方向）と、通信の可否を追加登録する（ステップS208、209）。この追加登録は、所定のデータベースを用いて自動的に登録されるようにしてもよいし、パケットフィルタリング情報アドレス変換情報表示/編集部42を介して管理者が追加登録するようにしてもよい。

【0089】つぎに、前記取り出したアクセス規則からこのアクセス規則に属する適用ドメインtoを取り出し（図14ステップS210）、この適用ドメインtoのドメイン名に対応する1～複数のホストアドレス（ローカルアドレス）を図4のドメイン定義テーブルT1から取り出す（ステップS211）。

【0090】つぎに、前記取り出したアクセス規則に属する適用ドメインfromを取り出し（ステップS212）、この適用ドメインfromのドメイン名に対応する1～複数のホストアドレス（グローバルアドレス）を図12のドメイン定義テーブルT1から取り出す（ステップS213）。

【0091】つぎに、適用ドメインtoの1～複数のホストアドレス（ローカルアドレス）を発信元アドレス/ポ

16

ート番号とし、適用ドメインfromの1～複数のホストアドレス（グローバルアドレス）を宛先アドレス/ポート番号とした全てのホストアドレスの組み合わせを何れかのファイアウォールのパケットフィルタリング情報としてパケットフィルタリング情報テーブルT4に登録する（ステップS214）。

【0092】図5の規則名PJ1-1の場合は、適用ドメインto（サーバドメインB）のホストアドレス（ローカルアドレス）がL103、L104で、適用ドメインfrom（端末ドメインA）のホストアドレス（グローバルアドレス）がG1であるので、L103→G1、L104→G1の2つのパケットフィルタリング情報がファイアウォールFW2用のものとして登録される。これら2つのパケットフィルタリング情報は、図16の下側の2つの欄に示されている。グローバルアドレスがG1の端末ドメインAはBasic NATでポート番号をアドレス変換の対象にしていないので、パケットフィルタリング情報が2個になっている。

【0093】つぎに、上記取り出したアクセス規則のプロトコル種別を図5に示すアクセス規則テーブルT2から取り出し、該取り出したプロトコル種別を上記登録したパケットフィルタリング情報にプロトコル種別として登録する（ステップS215）。さらに、登録したパケットフィルタリング情報に通信の方向（例えば双方向）と、通信の可否を追加登録する（ステップS216、217）。

【0094】ステップS220においては、図5に示すアクセス規則テーブルT2につきアクセス規則があるか否かが判定される。次のアクセス規則がある場合は、このアクセス規則に関して前記と同様の手順が行われることにより、読み出したアクセス規則に対応するパケットフィルタリング情報が作成され、作成されたパケットフィルタリング情報は前記同様にしてパケットフィルタリング情報テーブルT4に記憶される。

【0095】図5のアクセス規則テーブルT2に登録された全てのアクセス規則について、前述した処理を繰り返すことにより、図15および図16に示すような、各LAN12、13のファイアウォールFW1、FW2のパケットフィルタリング情報が作成される。

【0096】図5の規則名PJ1-2の場合は、適用ドメインfrom（端末ドメインB）のホストアドレス（ローカルアドレス）がL101、L102で、適用ドメインto（サーバドメインA）のホストアドレス（グローバルアドレス）がG3、G4であるので、L101→G3、L101→G4、L102→G3、L102→G4の4つのパケットフィルタリング情報がファイアウォールFW2用のものとして登録される。これら4つのパケットフィルタリング情報は、図16の上側の4つの欄に示されている。

【0097】さらに、図5の規則名PJ1-2の場合



(10)

特開2002-261788

17

は、適用ドメインcc（サーバドメインA）のホストアドレス（ローカルアドレス）がL3、L4で、適用ドメインfrom（端末ドメインB）のホストアドレス（グローバルアドレス）がG101であるので、L3→G101/\*、L3→G101/\*、L4→G101/\*、L4→G101/\*の4つのパケットフィルタリング情報がファイアウォールFW1用のものとして登録される。これら2つのパケットフィルタリング情報は、図15の下側の2つの欄に示されている。グローバルアドレスがG101の端末ドメインBはNAPTでポート番号をアドレス変換の対象にしているので、パケットフィルタリング情報が4個になっている。

【0098】このようにこの実施の形態においては、各LAN12、13の運用ポリシーとしてのドメイン定義テーブルT1、アクセス規則テーブルT2と、空グローバルアドレステーブルT5と、NAT設定規則テーブルT6と、サービス定義テーブルT7とに基づいて各LAN12、13のファイアウォールFW1、FW2で用いてNATアドレス変換情報D1b、D2bおよびパケットフィルタリング情報D1a、D2aを生成するようにしたので、NATを用いて複数のLAN間をインターネット接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。また、人間に判りやすい運用ポリシー定義を用いたので、専門知識も持たない者でもファイアウォールの設定情報を簡単に作成することができる。

【0099】なお、上記実施の形態においては、ネットワーク管理装置は、インターネットを介して接続される2つのLANを管理対象としたが、インターネットを介して接続される3つ以上のLANを管理対象にしてもよい。また、上記実施の形態においては、各LANには、1つの端末ドメインおよび1つのサーバドメインが含まれるようにしたが、前述したように、1つのLANに複数の端末ドメインおよび複数のサーバドメインが含まれるような網構成にも本発明は適用可能である。

【0100】

【発明の効果】以上説明したように、この発明によれば、複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を用いてNATアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、NATを用いて複数のLAN間をインターネット接続するための各ファイアウォールでの所要の設定情報を一括して簡単に自動作成することができるようになる。

【0101】つぎの発明によれば、端末とサーバとを別グループとして複数のグループに分け、該分けたグループ間でのアクセス規則を前記運用ポリシーとして前記データベースに蓄積しているので、人間に判りやすい運用ポリシー定義を用いることができ、専門知識も持たない

18

者でもファイアウォールの設定情報を簡単に作成することができる。

【0102】つぎの発明によれば、当該LANの1つの端末グループから他のLANの1つのサーバグループへのアクセスを単位として、管理すべき複数のLAN内に含まれる全ての端末グループおよびサーバグループについてのアクセス規則を登録するようにしているので、人間に判りやすい運用ポリシー定義を用いることができ、専門知識も持たない者でもファイアウォールの設定情報を簡単に作成することができる。

【0103】つぎの発明によれば、アクセス規則にグローバルアドレスの割当数がグループ毎に設定しているので、専門知識も持たない者でもファイアウォールの設定情報を簡単かつ正確に作成することができる。

【0104】つぎの発明によれば、アクセス規則に、プロトコル種別、サービス種別、同じグループ内での各端末の同時接続の有無が登録されているので、専門知識も持たない者でもファイアウォールの設定情報を簡単かつ正確に作成することができる。

【0105】つぎの発明によれば、端末およびサーバの区別、自グループ内の端末またはサーバの同時接続の有無、サービス指定ポート番号の有無などの登録情報に基づいてNAT種別が分類されるので、専門知識も持たない者でもNAT種別を簡単に分類することが可能になる。

【0106】つぎの発明によれば、サービス定義には、サービス種別、端末およびサーバの区別、指定ポート番号が登録されているので、専門知識も持たない者でもサービス定義を正確に登録することができる。

【0107】つぎの発明によれば、運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を編集し、該編集結果を前記データベースに登録する手段を備えているので、運用ポリシー、LANの構成などが変更された場合にもこれに容易に対処することができる。

【0108】つぎの方法発明によれば、複数のLANの運用ポリシー、各端末および各サーバのローカルアドレス、使用可能なグローバルアドレス、NAT設定規則、サービス定義に関する情報を用いてNATアドレス変換情報およびパケットフィルタリング情報を生成するようにしたので、NATを用いて複数のLAN間を接続するための各ファイアウォールでの所要の設定情報を一括して簡単に作成することができる。

【図面の簡単な説明】

【図1】 この発明を適用するインターネット接続の網構成の一例を示すブロック図である。

【図2】 この発明にかかるファイアウォール管理装置に内蔵される管理ソフトウェアの機能構成の一例を示したブロック図である。



(11)

特開2002-261788

19

20

【図3】 ファイアウォール接続ドメインテーブルの登録内容を例示する図である。

【図4】 ドメイン定義テーブルの登録内容を例示する図である。

【図5】 アクセス規則テーブルの登録内容を例示する図である。

【図6】 空グローバルアドレステーブルの登録内容を例示する図である。

【図7】 NAT設定規則テーブルの登録内容を例示する図である。

【図8】 サービス定義情報テーブルの登録内容を例示する図である。

【図9】 アドレス変換情報生成部で行われるアドレス変換情報作成処理の手順を示すフローチャートである。

【図10】 作成された一方のファイアウォールのアドレス変換情報を示す図である。

【図11】 作成された他方のファイアウォールのアドレス変換情報を示す図である。

【図12】 アドレス変換情報作成後のドメイン定義テーブルの登録内容を示す図である。

【図13】 パケットフィルタリング情報生成部で行われるパケットフィルタリング情報作成処理の手順（その一）を示すフローチャートである。

【図14】 パケットフィルタリング情報生成部で行われるパケットフィルタリング情報作成処理の手順（その二）を示すフローチャートである。

\*【図15】 作成された一方のファイアウォールのパケットフィルタリング情報を示す図である。

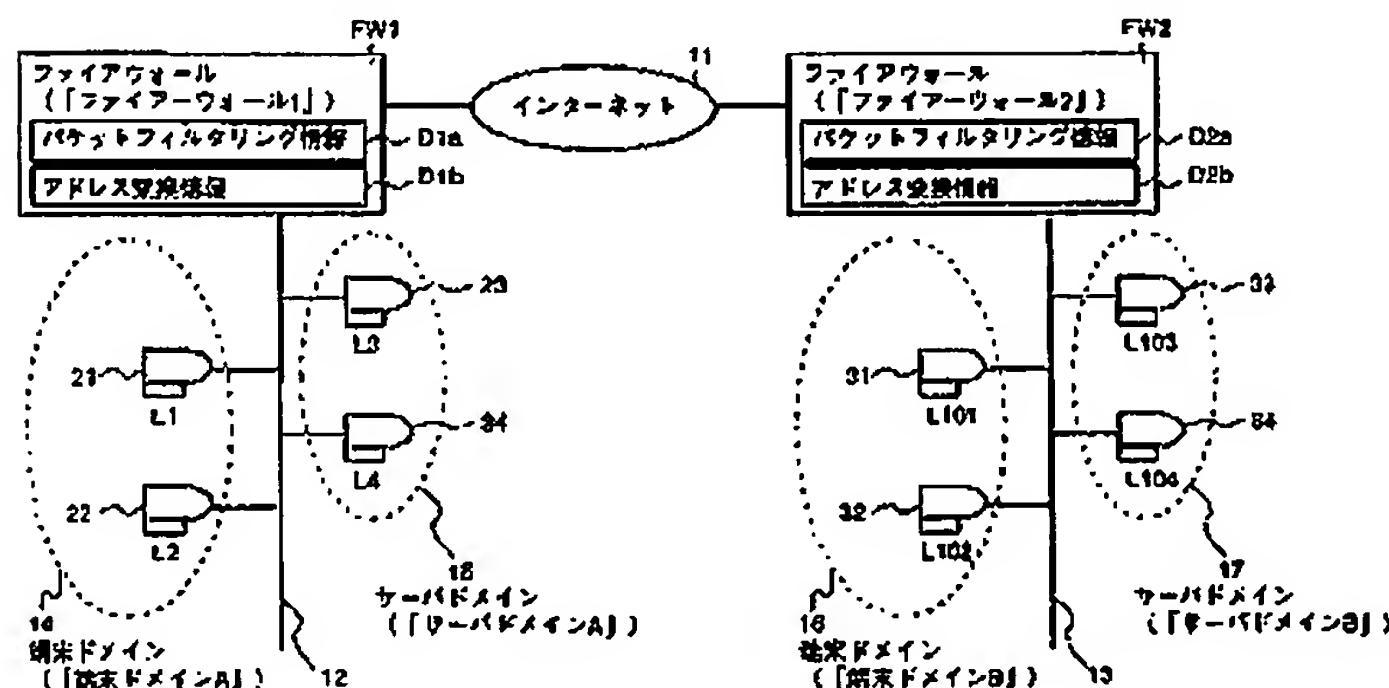
【図16】 作成された他方のファイアウォールのパケットフィルタリング情報を示す図である。

【符号の説明】

11 インターネット、 14 端末ドメイン、 15 サーバドメイン、 16 端末ドメイン、 17 サーバドメイン、 21 端末、 23 サーバ、 24 サーバ、 31 端末、 33 サーバ、 34 サーバ、 40 管理ソフトウェア、 41 ドメイン定義アクセス規則入力部、 42 パケットフィルタリング情報アドレス変換情報表示/編集部、 43 空グローバルアドレステーブル表示/編集部、 44 NAT設定規則サービス定義編集部、 45 アドレス変換情報生成部、 46 パケットフィルタリング情報生成部、 47 ファイアウォール接続ドメイン入力部、 D1a パケットフィルタリング情報、 D2a パケットフィルタリング情報、 D1b アドレス変換情報、 D2b アドレス変換情報、 FW1 ファイアウォール、 FW2 ファイアウォール、 T1 ドメイン定義テーブル、 T2 アクセス規則テーブル、 T3 アドレス変換情報テーブル、 T4 パケットフィルタリング情報テーブル、 T5 空グローバルアドレステーブル、 T6 NAT設定規則テーブル、 T7 サービス定義テーブル、 T8 ファイアウォール接続ドメインテーブル。

【図1】

【図6】



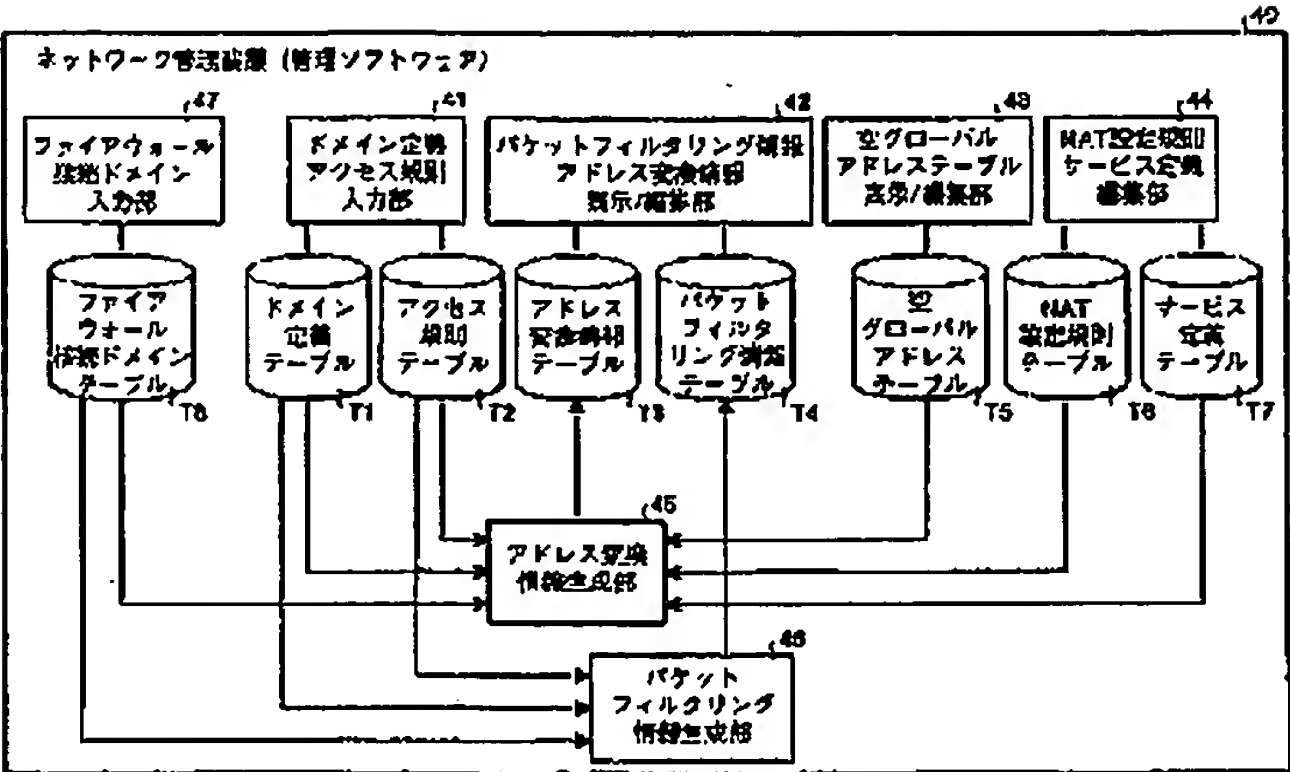
【図3】

【図4】

ファイアウォール接続ドメインテーブル		ドメイン定義テーブル	
ファイアウォール名	接続ドメイン	ドメイン名	ドメイン種別
ファイアウォール1	端末ドメインA、サーバドメインA	端末ドメインA	端末
ファイアウォール2	端末ドメインB、サーバドメインB	サーバドメインA	サーバ
		端末ドメインB	端末
		サーバドメインB	サーバ

(12) 特開2002-261788

【図2】



【図5】

【図7】

アクセス規則テーブル T2

規則名	適用ドメイン Dom		適用ドメイン D		プロトコル 種別	サービス 種別	接続同種接続
	ドメイン名	適用 アドレス数	ドメイン名	適用 アドレス数			
P21-1	端末ドメインA	1	サーバドメインB	-	TCP	FTP	なし
P21-2	端末ドメインB	1	サーバドメインA	-	TCP	FTP	あり

NAT設定規則テーブル T8

ドメイン種別	自ドメイン内での 変換同時接続	サービス指定 ポート番号	NAT種別
端末	あり	あり	BasicNAT
端末	あり	なし	NAPT
端末	なし	あり	BasicNAT
端末	なし	なし	NAPT
サーバ	あり	あり	StaticNAT
サーバ	あり	なし	StaticNAT

【図8】

【図10】

サービス 定義情報テーブル T7

サービス種別	ドメイン種別	指定ポート番号
FTP	端末	なし
FTP	サーバ	21 (制御コネクション) 20 (データコネクション)

ファイアウォールFW1

アドレス交換情報 D1b

ローカルアドレス/ポート番号	グローバルアドレス	NAT種別
L1/L2*	G1/-	BasicNAT
L3*	G3/-	StaticNAT
L4/*	G4/-	StaticNAT

【図11】

【図12】

ファイアウォールFW2

アドレス交換情報 D2b

ローカルアドレス/ポート番号	グローバルアドレス	NAT種別
L101/L102/*	G101/-	NAPT
L103/*	G103/-	StaticNAT
L104/*	G104/-	StaticNAT

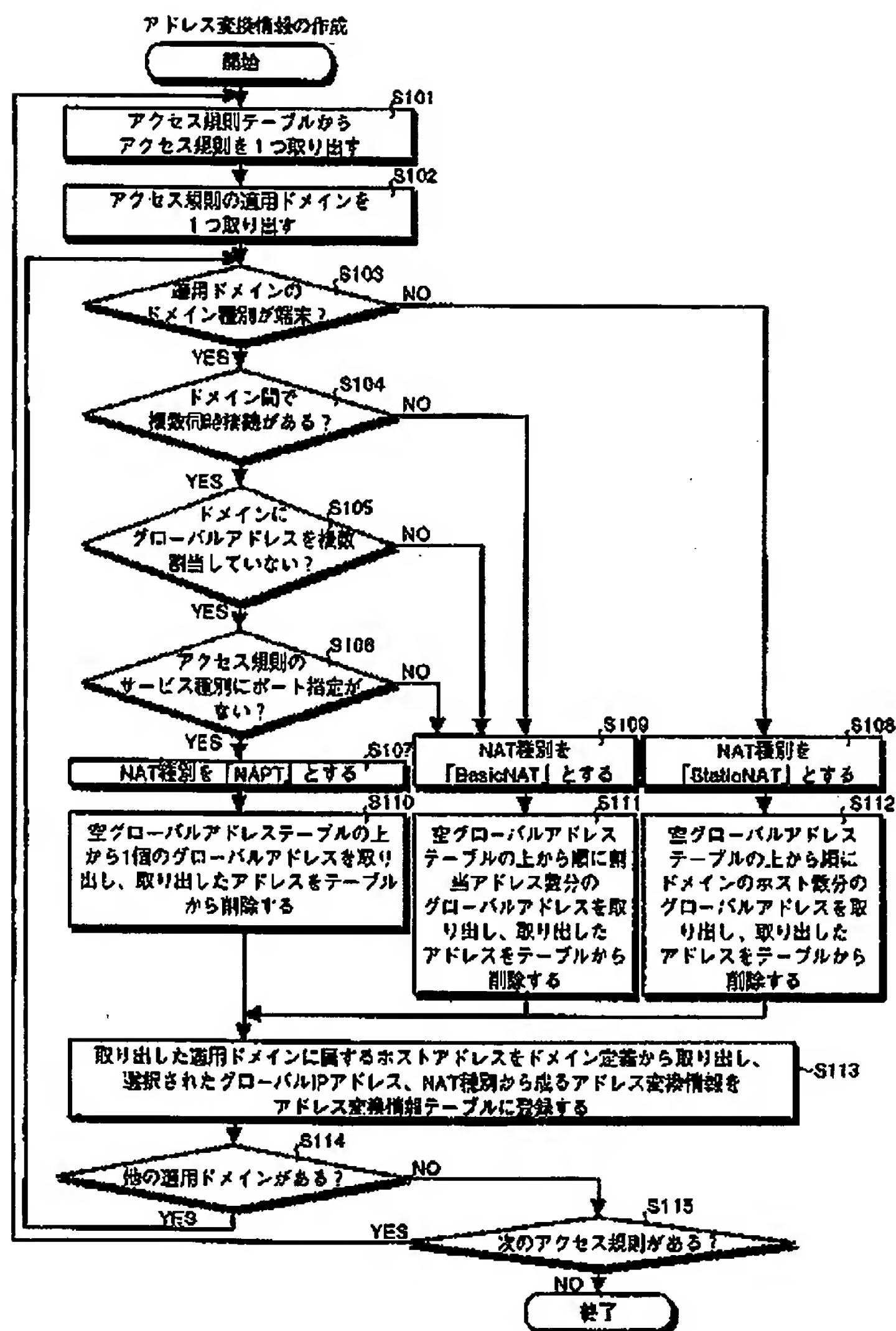
ドメイン定義テーブル T1

ドメイン名	ドメイン種別	ホストアドレス (ローカルアドレス)	ホストアドレス (グローバルアドレス)
端末ドメインA	端末	L1/L2	G1
サーバドメインA	サーバ	L3	G3
		L4	G4
端末ドメインB	端末	L101/L102	G101
サーバドメインB	サーバ	L103	G103
		L104	G104

(13)

特開2002-261788

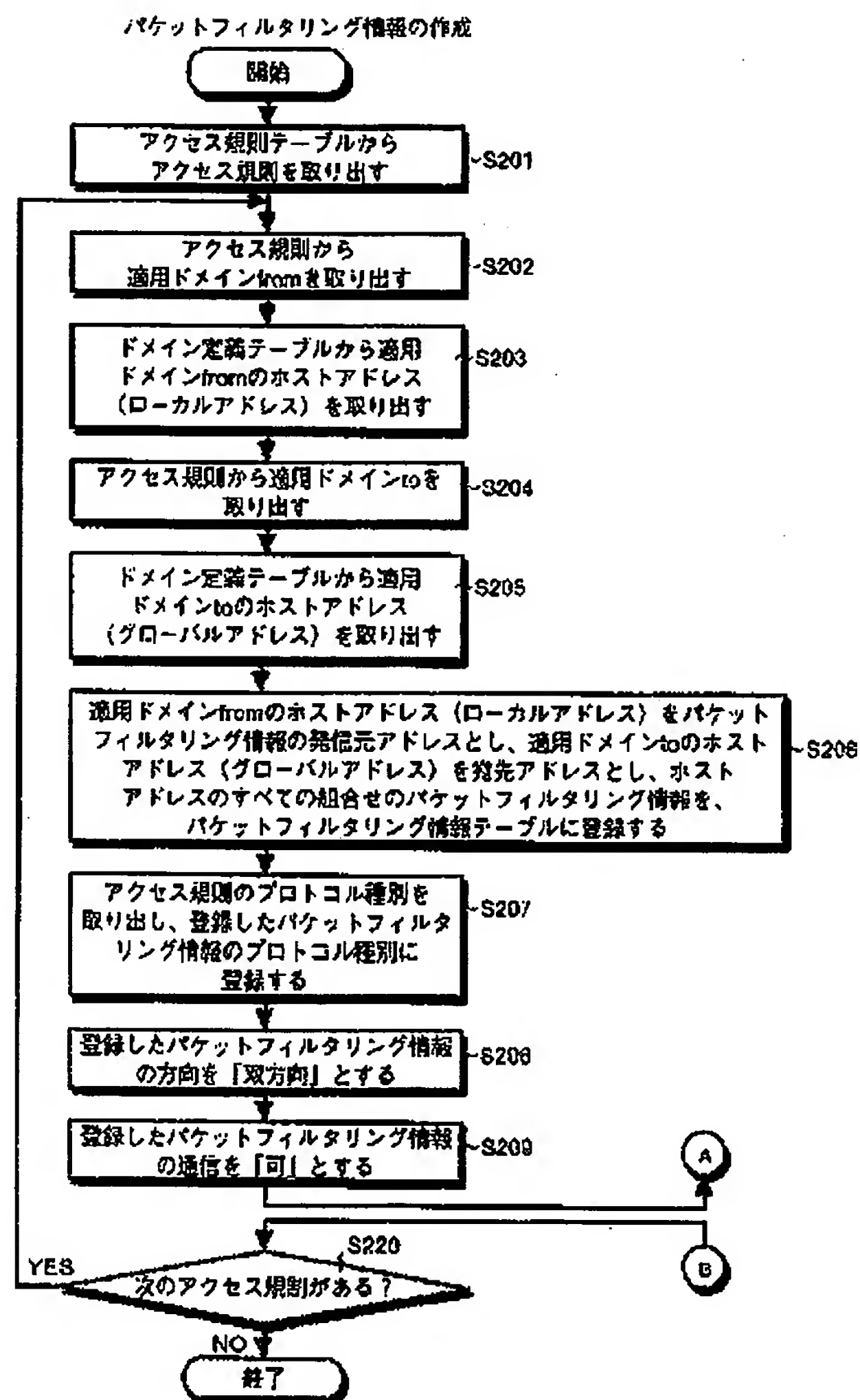
【図9】



(14)

特開2002-261788

【図13】

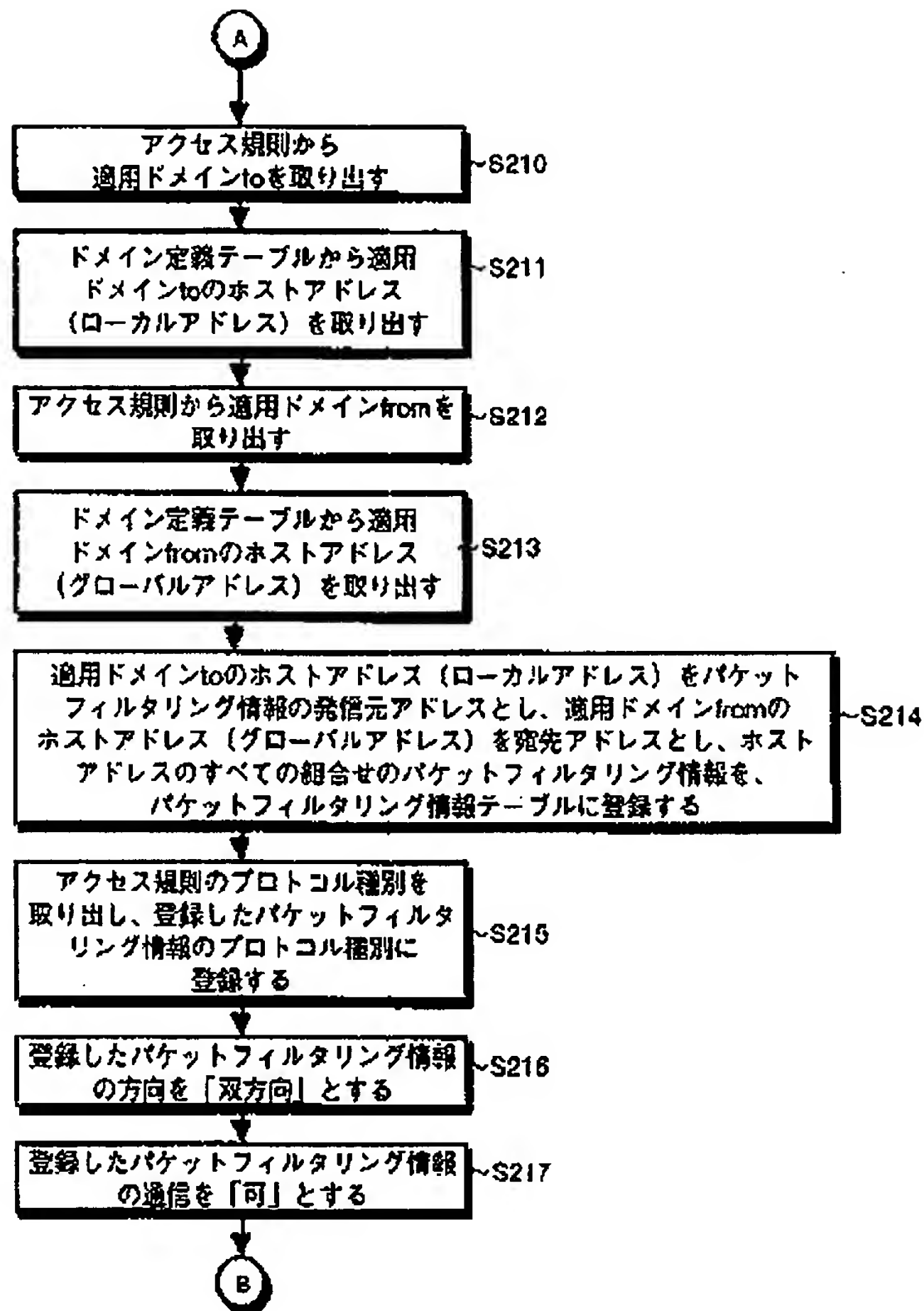




(15)

特開2002-261788

【図14】



【図15】

ファイアウォールFW1

パケットフィルタリング情報 01a

発信元アドレス/ポート番号	宛先アドレス/ポート番号	プロトコル種別	方向	通信
L1/*	G102/*	TCP	双方向	可
L1/*	G104/*	TCP	双方向	可
L2/*	G103/*	TCP	双方向	可
L2/*	G104/*	TCP	双方向	可
L3/*	G101/*	TCP	双方向	可
L3/*	G101/*	TCP	双方向	可
L4/*	G101/*	TCP	双方向	可
L4/*	G101/*	TCP	双方向	可

【図16】

ファイアウォールFW2

パケットフィルタリング情報 02a

発信元アドレス/ポート番号	宛先アドレス/ポート番号	プロトコル種別	方向	通信
L101/*	G3/*	TCP	双方向	可
L101/*	G4/*	TCP	双方向	可
L102/*	G3/*	TCP	双方向	可
L102/*	G4/*	TCP	双方向	可
L103/*	G1/*	TCP	双方向	可
L104/*	G1/*	TCP	双方向	可